Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for year: 2009

Date Filed: February 26, 2010

Name of Company covered by the certification: Communication Options, Inc.

Form 499 Filer ID: 812048

Name of signatory: Stephen K. Vogelmeier

Title of signatory: President

I, Stephen K. Vogelmeier, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions against data brokers in the past year. The company has no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available (*e.g.,* through new media), regarding the processes pretexters are using to attempt to access CPNI.

The company has not received any customer complaints in the past year concerning unauthorized release of CPNI.

Signed: 

Stephen K. Vogelmeier

President, Communication Options, Inc.

Customer Proprietary Network Information Certification

Attachment A

COI has established practices and procedures adequate to ensure compliance with Section 222 of the Communication Act of 1934, as amended and the Federal Communications Commission's (FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in Sections 64.2001 – 64.2011 of the Commission's rules. This attachment summarizes those practices and procedures.

Safeguarding against pretexting

- COI takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI based on customer-initiated contacts. COI is committed to notifying the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against protesters and data brokers.

Training and discipline

- COI trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out COI;s obligation to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, (d) obtain customers' informed consent as required with respect to its use for marketing purposes, and (e) keep records regarding receipt of such consent, customer complaints regarding CPNI and the use of CPNI for market campaigns.
- COI employees are required to review COI's CPNI practices and procedures and to acknowledge receipt and review thereof.
- COI also requires all outside Dealers and Agents to review COI's CPNI practices and procedures and to acknowledge receipt and review thereof.
- COI has a disciplinary process in place for violation of the company's CPNI practices and procedures. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

COI's use of CPNI

- COI may use CPNI for the following purposes:
    - To initiate, render, maintain, repair, bill and collect for services;
    - To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
    - To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent;
    - To market additional services to customers that are within the same categories of service to which the customer already subscribes;
    - To provide CPE and call answering, voicemail or messaging, voice storage and retrieval services, fax store-and-forward, and protocol conversion;
    - To market services formerly known as adjunct-to-basic services; and
- COI does not disclose or permit access to CPNI to track customers that call competing providers.
- COI discloses and permits access to CPNI where required by law (e.g., under a lawfully issued subpoena).
- COI maintains CPNI no longer than necessary for its original purpose, except when required to maintain CPNI by law or for any legitimate business purpose.

- COI does not market or otherwise sell CPNI to any third party.

Customer approval and informed consent

- COI has implemented a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This system also allows for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.
    - Prior to any solicitation for customer approval, COI notifies customers of their right to restrict the use of, disclosure of, and access to their CPNI.
    - COI uses opt-in approval when using or disclosing CPNI for purposes other than permitted under opt-out approval or in 47 USC 222 and the FCC's CPNI rules.
    - A customer's approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval.
    - Records of approvals are maintained for at least one year.
    - COI provides individual notice to customers when soliciting approval to use, disclose, or permit access to CPNI.
    - The content of COI's CPNI notices comply with FCC rule 64.2008(c).

Opt-out

- COI uses opt-out for the marketing of communications related services by its employees outside the category of service to which the customer subscribes and for affiliate marketing of any communications related services. When COI uses opt-out approval, COI provides notification by electronic or written methods and waits at least 30 days after sending customers notice (for mail notifications, the 30 days begins to run 3 days after the notice was sent) and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. COI provides customers with opt-out notifications every two years. When using e-mail for opt-out notices, COI complies with the additional requirements set forth in FCC Rule 64.2008(d)(3). Additionally, COI makes available to every customers an opt-out method, at no additional charge, that is available 24 hours a day, seven days a week.

Opt-in

- COI uses opt-in approval for marketing by independent contractors and joint venture partners and for the marketing of non-communications related services by itself and its affiliates. When COI uses opt-in approval, COI provides notification consistent with FCC Rule 64.2008(c).

One time use

- After authentication, COI uses oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice comports with FCC Rule 64.2008(f).

Additional Safeguards

- COI maintains for at least one year records of all marketing campaigns that use its customers' CPNI, including a description of each campaigns are subject to a supervisory approval and compliance review process the records of which also are maintained for a minimum of one year.
- COI has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules for outbound marketing situations and maintenance of records.
- COI designates one or more officers, as an agent or agents of the company, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in FCC Rule 64.2009(e)
- COI will provide written notice to the Commission in accordance with the requirements of FCC Rule 64.2009(f) if ever its opt-out mechanisms malfunction in the manner described therein.

- For customer-initiated telephone inquiries regarding or requiring access to CPNI, COI authenticates the customer (or its authorized representative), through a pre-established password, without prompting through the use of readily available biographical or account information. If the customer cannot provide a password, then COI only discloses call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number or record.

- For online customer access to CPNI, COI authenticates the customer (or its authorized representative) without the use of readily available biographical or account information. After the customer has been authenticated, COI utilizes a customer-established password to authorize account access. COI establishes passwords and has employed back-up authentication for lost or forgotten passwords consistent with the requirements of FCC Rule 64.2010(e).

- COI does not have any retail locations.

- COI notifies customers immediately of any account change, including address of record, authentication, online account and password related changes.

- COI may negotiate alternative authentication procedures for services that COI provides to business customers that have both a dedicated account representative and a contract that specifically addresses COI's protection of CPNI.

- In the event of a breach of CPNI, COI will notify law enforcement as soon as practicable, no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs COI to delay notification, or COI and the investigatory party agree to an earlier notification. COI will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with the notifications sent to law enforcement and affected customers.

- When COI discloses to or provides independent contractors or joint venture partners with access to CPNI, it does so pursuant to confidentiality agreements that (a) require the independent contractor/joint venture partner to use CPNI only for the purpose it has been provided, (b) prohibit independent contractor/joint venture partners disclosure of such CPNI except under force of law, and (c) require the independent contractor/joint venture partner to have appropriate protections in place to ensure the ongoing confidentiality of the CPNI.